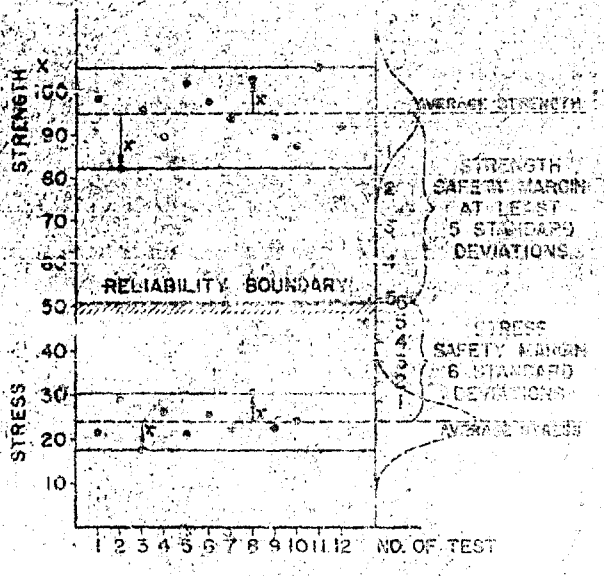
Reliability Through Safety Margin



October 1958

Research And Development Division
Army Rocket And Guided Missile Agency
Redstone Arsenal, Alabama

RELIABILITY
THROUGH SAFETY MARGINS

OCTOBER 1958

By Robert Lusser
ROBERT LUSSER

ABSTRACT

To make complex military equipment satisfactorily reliable, present specifications are totally inadequate. It is imperative that generous safety margins between "stresses" and "strengths" be specified, applied, and controlled by the contracting agencies.

A Reliability Code, consisting of 21 paragraphs, is formulated to supplement and override existing specifications.

This study is an expanded version of an earlier paper "Reliability Specifications for Guided Missiles," by the same author.

Table of Contents

INTRODUCTION

There is a widespread belief that reliability requirements are very much the same for guided missiles as for piloted aircraft, because "both are airborne." This is a dangerous mistake. Both are airborne, true, and both are complex. But they differ in one significant respect: *the "vital" complexity,* which is not indicated by the number of *all* components, but by the number of vital components — those that by their failure will cause the total loss of the missile or the aircraft.

In commercial piloted aircraft, only a few dozen components, most of them structural, are really vital in the sense that failure of any one of them will cause a total loss. Thousands of other components, particularly the electronic components, are not vital. They may fail, and they do fail, without any catastrophic consequences because the pilot can do without them and bring the aircraft safely home for inspection and repair.

In guided missiles, on the other hand, *all* components, *including electronic components,* are vital since any one of them, if it fails, will invariably cause the missile to miss its target. A missile once fired cannot be recovered, repaired, and re-used like a piloted aircraft. If it does not hit its target, the loss is complete—both in taxpayers' dollars and in potential military consequences.

If we compare the number of vital components of a piloted aircraft and a missile, we realize why *piloted aircraft are orders of magnitude, perhaps a thousand times, more reliable than guided missiles. Obviously, as far as the achievement of reliability is concerned, guided missiles and piloted aircraft belong in entirely different categories.*

Since World War II, the "vital" complexity of non-missile equipment such as radar, commercial piloted aircraft, and computers has steadily increased. Yet, apparently, these categories of equipment continue to be satisfactorily reliable. If this were not so, no one would dare board an airliner, and no computer would be of any use.

This rather favorable situation is illustrated by the lower curve in Figure 1 representing the growth of "vital" complexity in non-missile equipment since 1935. The growth has been slow, hence the increase in component reliability has kept pace with it.

Now compare that line with the breathtaking climb of the upper curve in the diagram. This curve represents the growth in complexity of non-recoverable equipment: ammunition, bombs, mines, torpedoes, missiles, guided missiles and unmanned satellites. Here complexity is rapidly outgrowing the state of the art of making components reliable. Thus, an ever-increasing deficit is created between the reliability level of ordinary components and the level required to attain an acceptable overall reliability.

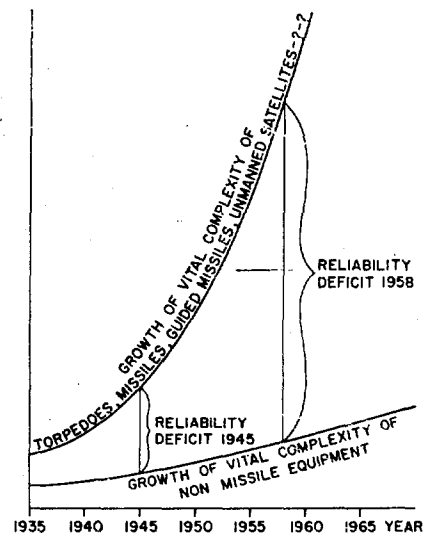


Fig. 1. Trend of Complexity of Recoverable and Non-recoverable Equipment Indicated by the Number of Vital Components

Unfortunately, as new performance requirements accelerate this upward trend of complexity, the deficit increases year by year, with the end nowhere in sight.

Obviously, if we want to make complex military equipment satisfactorily reliable, this dangerous trend must be stopped, and even reversed. How this may be accomplished is the subject of this study.

PART I

THREE CATEGORIES OF RISK

There are many fallacious concepts of quality and reliability which contribute to the unreliability of complex equipment. One by one they lose ground. One of these concepts, however, is still deeply entrenched in the routines of design, manufacture, and procurement: that components which comply with standard specifications may safely be employed in all kinds of equipment, be they simple or complex, inexpensive or costly, harmless or fraught with heavy risks.

This fallacious concept completely ignores the *consequences of failure.* If consequences are harmless, unreliability poses little or no problem. However, if they are serious, or very serious, the achievement of reliability may become the overriding problem of design, manufacture, maintenance, and operation.

Degrees of risk caused by unreliability vary tremendously, ranging from no risk at all, as in home radios, to extremes of risk, as in atomic bombs and spaceships. Obviously, components of a spaceship must be made much more reliable than those of a home radio.

How much more reliable? Ten, or a hundred, or a thousand times? This question cannot be answered conclusively because actual figures depend on individual cases. But, to permit at least a rough appraisal of the required reliability effort, the following three classes of equipment may be established:

(a) ***Low-Risk Equipment:*** That which in the event of failure can always be repaired and put to work again. Examples: home appliances and office machines. For such equipment, commercial standards of quality may be stringent enough to achieve and control quality and reliability.

(b) ***High-Risk Equipment:*** A very costly equipment which, in the event of failure of any one of its components, is irretrievably lost. Guided missiles are characteristic for this class. To make a high-risk equipment reasonably reliable, its components must be made perhaps *two orders of magnitude* (or a hundred times) more reliable than components for commercial use.

(c) ***Ultrahigh-Risk Equipment:*** That which, in the event of failure, will result not only in huge material losses, but also in loss of life, and perhaps national prestige. Example: A manned spaceship. Components to be employed in ultrahigh-risk equipment must be made perhaps *four orders of magnitude* (or ten thousand times) more reliable than commercial components.

By now it is widely appreciated that the overall reliability of a weapon system can be improved by increasing the reliability of its components. However, by establishing the above three classes of equipment risk we are forewarned to think of component improvements not by factors of two, three, or five, but by *orders of magnitude.* This, in turn, means that we must strive for an *absolute* degree of component reliability, and nothing less.

How can absolute component reliability be achieved? Many different efforts may be directed to this end. One of the most powerful of these is that of specifying generous safety margins between stresses and strengths.

It is a strange phenomenon that writers of military specifications thus far have failed to adopt the principle of safety margins. It therefore appears necessary that the intricate problem of specification writing be discussed first.

PART II

PRINCIPLES OF RELIABILITY SPECIFICATIONS

1. The Evolutionary Approach

It is argued that the overall reliability of a piece of equipment may best be raised by routinely revising and improving existing specifications.

Let us examine this argument carefully. Most specifications are the result of decades of cumbersome and costly trial and error. We call this *advancement of the state of art by evolution.* For example, we know that at least two piston

rings are required to seal and lubricate the pistons of a reciprocating engine. We know the most suitable material, the proper tolerances, and the most effective method of manufacture. We know also that we may expect a certain wear-out life, say 2,000 hours.

In a mature state of art such as this, contracting agencies can write clear-cut specifications for competitive bidding, design, production, quality control, and acceptance inspection. The contractor knows exactly what is required. By strictly adhering to these specifications he may achieve the specified quality, and even exceed it.

Not so with the components of complex military equipment, such as guided missiles. Their environmental conditions are often extremely severe and also little known. Hence their state of the art is far less mature and their reliability much lower.

But even if all conditions were perfectly known, and properly taken care of, present specifications still would be inadequate for achieving a satisfactory degree of overall reliability for the following reason: The overall reliability of a piece of complex equipment does not equal the *average* reliability of its components, as many still may think; it equals the *product* of them, as indicated by the reliability formula:

$$P_{overall} = p_1 \cdot p_2 \cdot p_3 \cdots p_n$$

According to this formula, to make a complex equipment reasonably reliable, its components must be made more reliable *in proportion to the "vital" complexity.* (A component is vital if its failure causes the loss of the whole equipment, and/or the death of a crew.) The vital complexity of a missile system, for example, may be a hundred times or a thousand times higher than the vital complexity of a commercial piloted aircraft. Hence, missile components must be made a hundred times or a thousand times more reliable than their commercial counterparts.

Present specifications neglect this fact entirely, just as they neglect the reliability formula. They demand only "quality" which, however, is a property *independent of complexity.* Small wonder then, that designers often work in the dark, torn by conflicting concepts of quality and reliability.

This is a serious handicap. Ammunition, mines, torpedoes, and missiles cannot be better than the specifications for their design and manufacture. Specifications should, therefore, be kept abreast or, if possible, ahead of the state of the art. Actually, they are lagging most of the time, thereby freezing the state of art at levels of reliability attained years ago. Attempts to tighten up the specifications are often opposed by persons and agencies who are responsible for speedy and economical production. But, speed and economy of production are archenemies of reliability. Therefore the progress in overall reliability, based on the evolution of ordinary specifications, is very slow.

There is another reason why the evolutionary approach in specification writing is utterly inadequate: The number of specification paragraphs that must be considered in the development and manufacture of guided missiles and their components is staggering; they cover more than 75,000 printed pages! To even read them may take years. To revise them with the intent to improve reliability may take a generation. Meanwhile, the complexity of military equipment may continue to climb far beyond any increase in component reliability that evolution can accomplish.

This does not imply that existing specifications are useless and should be discarded. They represent the state of art and should, therefore, always be consulted. At the same time, however, they should be mistrusted, because they were written for achieving the moderate degree of reliability required for commercial components, and by no means for achieving the "absolute" degree of component reliability required in highly complex military equipment.

2. The Revolutionary Approach

The question arises: Will we ever be able to establish an adequate state of art for all of the

thousands of component types employed in complex military equipment? The answer is yes. However, this can be brought about only by a *revolution* in specification writing. A radically new approach must be sought, based on those factors which actually govern reliability, namely:

a. The actual maximum environmental conditions occurring in service.

b. The actual mechanics of failure.

c. The actual ultimate strength with regard to each mechanics of failure.

d. The actual variation of strength.

e. The actual safety margin between average strength and environmental condition.

The writing of such reliability specifications supplementing and overriding conventional specifications is imperative. To these we turn now.

PART III

RELIABILITY THROUGH SAFETY FACTORS AND SAFETY MARGINS

1. The Principle of Safety Factors

To provide a safeguard against unpredictable stress levels that may cause failures, it is common practice to specify minimum safety factors between the ultimate strength of a component type and the maximum stress to which it may be exposed in service.

Exceptionally high safety factors are specified whenever human life is at stake, as in the structural designs of buildings, bridges, elevators, and aircraft. The minimum safety factors specified in the design of structures are shown in the excerpt from Machinery's Handbook, Figure 2.

The reader will note that the *factor of ignorance* should occasionally be given as high as 10!

In much the same manner, nature has endowed living organisms with amazingly high safety factors. Our heart can pump ten times the normal rate of blood flow; our lungs can exchange ten to twelve times the normal volume of air; our bones break at loads ten to twenty times the static loads.

Total Safety Factor $F = a \cdot b \cdot c \cdot d$

a — the ratio of ultimate strength to elastic limit (between 1.5 and 2).

b — depends on character of stress; 1 for a dead load; 2 for a load varying between zero and maximum; 3 for a load alternating between negative and positive.

c — depends on the manner in which loads are applied; 1 for load gradually applied; 2 for load suddenly applied; 3 and more for impact loads.

d — the factor of ignorance. Whereas the other factors provide against known conditions, this provides against the unknown. It varies between 1.5 and 3, it should occasionally be given as high a value as 10.

Example of a Piston Rod: $F = 2 \cdot 3 \cdot 2 \cdot 1.5 = 18$

Fig. 2. Specified Minimum Safety Factors in the Design of Structures and Machinery

Such generous safety factors have helped make structures and machines absolutely reliable, not just in their components but as whole complex systems. Example: The complex airframes of aircraft to which, without hesitation, we trust our lives.

It thus appears a matter of course that in guided missiles, too, generous safety factors should be specified and applied. Unfortunately, in some quarters the principle of safety factors is not appreciated. It is argued that generous safety factors would so encumber airborne equipment as to ruin its performance; that components which comply with conventional specifications are good enough to "assure" reliability; that there is no need to determine safety factors by tests to failure; and that the principle of safety factors is "nebulous anyway." It will be shown later in this study that these arguments, except for the first one, are invalid.

In rare instances, a safety factor of 1.5 is specified. It has been adopted from specifications for structures. However, this low safety factor takes care of only the known strength variation *of the basic materials,* and not of the many additional uncertainties and contingencies which plague the components of complex military equipment. Therefore, it is not nearly high enough to achieve the required degree of absolute component reliability.

There is another serious shortcoming of present specifications. To prove that safety factors are as specified, samples must be *tested to failure* with regard to any critical design characteristic, including wear-out life. However, present specifications rarely require tests to failure, *only tests up to specified limits.* Many of these limits were conceived years ago, by people who were in no position to know the extreme environmental conditions and the extreme reliability requirements of modern military equipment. Hence, most of the limits have become unrealistic and misleading.

Moreover, since failure tests are not required, component designers are not compelled to determine the inherent weaknesses of their creations, their ultimate strength values, and their safety factors. As a result, systems designers, employing the components in their systems, may never know whether they are highly reliable, marginal, or downright unreliable.

Considering the striking benefits derived from generous safety factors, one might wish that the presently specified low safety factor of 1.5 be raised drastically, say to four or five. This, however, cannot be recommended because it would, indeed, so encumber airborne equipment as to ruin its performance.

2. The Principle of Safety Margins

It would be ideal to have specifications which would increase both reliability and performance. We may attain this goal by replacing the principle of rigidly specified *safety factors* by the more sophisticated yet much more effective principle of *safety margins.* It takes care of the fact that *unreliability is caused not only by low averages but also by large variations of strength.*

Variations may be large or small, as illustrated in Figure 3. Although components A and B have the same average strength, component B evidently is far less reliable than component A. It is, therefore, imperative that the characteristic variation of stresses and strengths be determined also, by testing small but sufficient samples to failure. The result of such a test-to-failure program is illustrated in Figure 4.

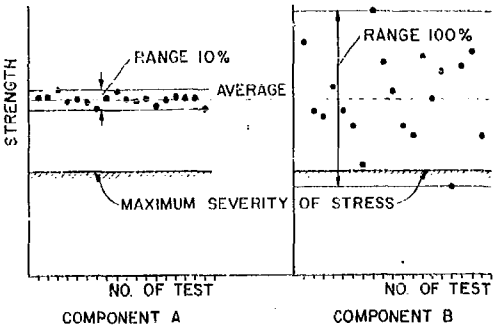


Fig. 3. Two Types of Components Exhibiting Different Variations of Ultimate Strengths

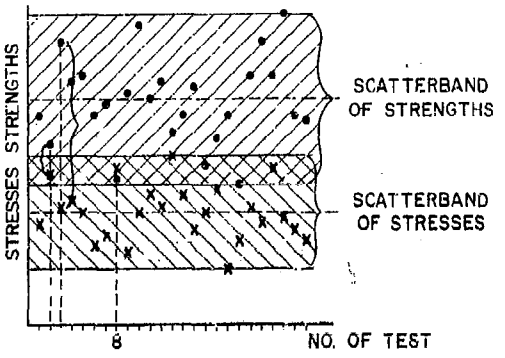


Fig. 4. Scatterbands of Stresses and Strengths

The reader will note that component No. 8 is weaker than the stress to which it will be subjected, and that therefore missile No. 8 will fail.

Obviously, scatterbands of stresses and strengths must be separated by *safety margins.* Here the question arises how large the safety margins should be to achieve the required ultrahigh, or "absolute," degree of component reliability.

Before we may discuss this vital question, we must dwell for the moment on the still-widespread misconception that reliability may be judged on the basis of a single failure test.

Figure 4 indicates that safety factors fluctuate even more violently than the stresses and strengths upon which they are based (compare Tests No. 2 and 3). Therefore, relying on the test-to-failure data of just one unit is short-

sighted and irresponsible. This is illustrated in Figure 5 where the scatterband of stress data has been replaced by the maximum stress level, called the "Reliability Boundary." (About Reliability Boundary, see Reference 1, Part V.)

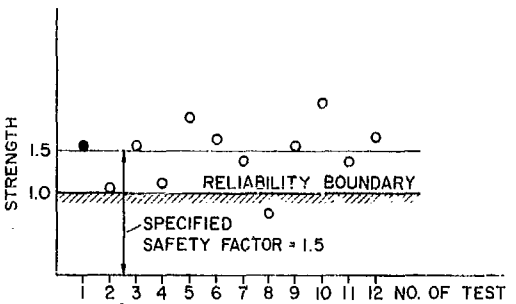


Fig. 5. The Fallacy of Testing Just One Unit

If only one test were conducted and relied upon, and if the result complied with the specified minimum safety factor of 1.5, as illustrated by the black dot, the component type might be accepted for mass production and employment in complex military equipment. If, however, more units were tested to failure, a shocking degree of variation, hence unreliability, would be revealed. The component type of Figure 5 may ruin not just missile No. 8 but many missiles, even a whole missile project.

3. Measuring Safety Margins

By testing a sufficient number of units up to failure, we obtain the characteristic variation of the strength data. We may express it in terms of the Range, or the Mean Deviation, or the Standard Deviation.

Which one of these three measures of variation is most suitable here? In Reference 2, page 287, it is shown that the standard deviation is far more efficient than the range, and approximately 10 per cent more efficient than the mean deviation. Ten per cent of a comprehensive test-to-failure program that may cost millions of dollars, would represent a substantial saving of money and time. Compared to this, the small extra effort required for computing the sample standard deviation is entirely negligible. It is therefore recommended that the standard deviation be used here.

Using the standard deviation as a yardstick of variability has a great advantage in that it permits the reliability engineer to tie in quality control with reliability control. We shall return to this problem in Section 6.

It has been argued that the standard deviation, being an accurate statistical tool, must not be employed as a measure of inaccurate safety margins. This argument is based on the erroneous assumption that the goal of reliability efforts is the *accurate measurement* of reliability, whereas in fact it is the *achievement* of reliability. For the components of complex military equipment this reliability must be so high that it cannot be measured anyway.* But it may be expressed indirectly by the number of standard deviations available between average strength and maximum stress. True, safety margins are inherently inaccurate, but this is no reason to deny the reliability engineer a mathematical tool, accurate or inaccurate, if it serves his purpose.

4. How to Judge and Increase Safety Margins

The principle of safety margins is illustrated by the examples shown in Figures 6 through 10.

Let us assume that between the average strength and the Reliability Boundary a minimum safety margin of five standard deviations were specified. After having tested a sample, say 12 units, to failure we compute the standard deviation and find that the safety margin is only 2.7 standard deviations (Figure 6). Thus, the safety margin must be increased. We may first try to lower the severity of the environmental condition, for example by pro-

*As a rule of thumb, the sample size must be 10 times as large as indicated by the permissible reciprocate failure rate if we want to prove, with a confidence of 90 per cent, that the real probability of failure lies between 0.5q and 1.5q (where q is the measured failure rate). For example, if we want to prove that not more than one unit out of a hundred will fail, we must test a thousand units. If we want to prove that not more than one unit out of a hundred thousand will fail--this may be required for the components of complex guided missiles we must test a million units of each type of component! (See "Testing to Specified Limits Versus Testing to Failure," by this author.)

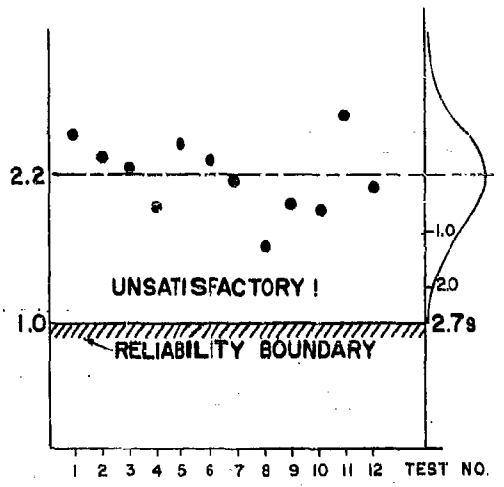


Fig. 6

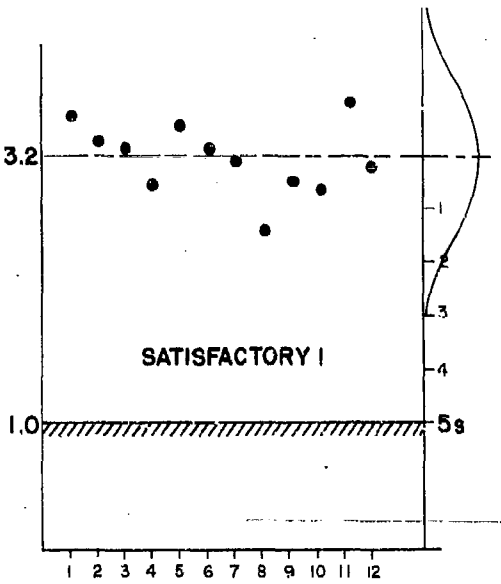


Fig. 7

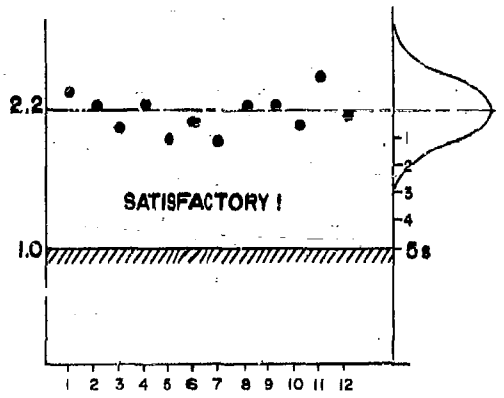


Fig. 8

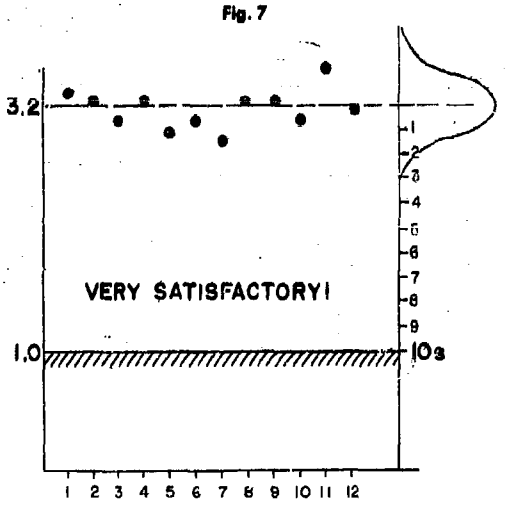


Fig. 9

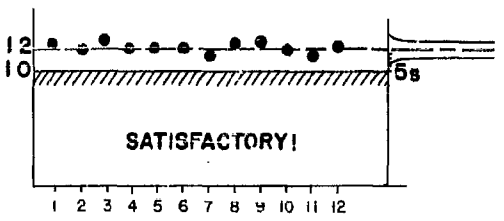


Fig. 10

viding a shock absorber or by intensifying the cooling of the component. We may also select a stronger type of component. If neither is practical, the component must be redesigned. In most instances, this is easy because the failure tests will have revealed the prevailing modes, or mechanics, of failures. Either the average strength may be increased, as shown in Figure 7, or the inherent variation reduced, as in Figure 8, whichever appears most suitable to save weight, time, or expense.

Redesign may result in an increase of the average strength, or in a decrease of variation, or both. In the latter case, the safety margin may soar up to 10 standard deviations, as shown in Figure 10, twice as many as specified, and almost four times as many as attained initially---a great achievement!

Whenever saving of weight is not a paramount issue, large safety margins are highly welcome contributions to the overall reliability. Therefore, in specifying safety margins we should be generous. We should use a shovel rather than a scalpel: Ten standard deviations are preferable to five, and 20 preferable to 10.

Components having very large safety margins may be considered "absolutely" reliable. They may be placed in the "'good' basket," thereby freeing us to concentrate on those component types which still suffer from low safety margins.

When saving of weight is of prime importance, as in the design of structural components, the concept of safety margins permits saving weight by keeping the safety margin down to the specified minimum of, say, five standard deviations. (Compare Figure 9 to Figure 8.) In the design of simple structural parts having very small inherent variations of strength, such as machined pins, the designer may reduce dimensions and weight to a bare minimum if he can prove, through tests to failure, that the specified minimum safety margin of, say five standard deviations, is still available.

This is illustrated in Figure 10. Although, in this event, the safety *factor* is only 1.2, the component may be accepted, and *considerable weight may be saved.* It thus becomes evident that the principle of safety margins not only helps to achieve and control the required "absolute" degree of component reliability, but also helps to improve *performance* by indicating where dead weight may be saved. *Thus the crucial antagonism between performance and reliability may be greatly alleviated.*

5. Strength Testing Versus Life Testing

Many believe that the principle of safety margins is applicable to strength testing, but not to life testing. Thus a conceptual discrepancy is created, resulting in a great deal of unnecessary confusion.

Actually, as discussed in the Introduction of Reference 1, the terms "stresses" and "strengths" are not restricted to mechanical forces; they may be applied to life as well. *Strength* of life is indicated by a scatterband of life test data, whereas *stress* of life is indicated by the specified *replacement age.*

This is illustrated by the characteristic wear-out frequency distribution, Figure 11. To assure that a piece of equipment will not fail from wear-out, its components must be replaced *preventively,* that is, before the wear-out distribution hump is reached. To this end, a minimum safety margin between the average life and the replacement age must be specified, as shown in Figure 11. Again, this safety margin may best be expressed in standard deviations. The reader will notice that the specified replacement age constitutes the Reliability Boundary.

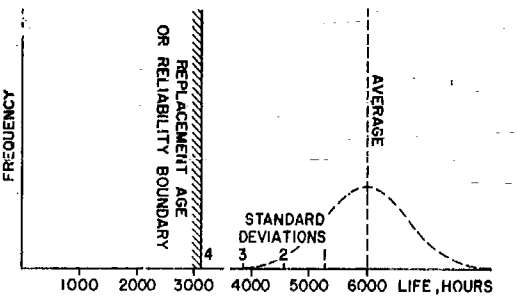


Fig. 11. Safety Margin Between Mean Life and Replacement Age

Life safety margins may be increased by simply lowering the specified replacement age. This is generally easier than lowering the severity of an environmental stress condition. However, it will increase cost of maintenance.

As in strength testing, the sample sizes required in life testing need not be large. Twenty, ten, or even fewer units may occasionally suffice to obtain a rough picture of the average life, and the variation of life.

Small sample sizes such as these bring about a great deal of statistical uncertainty. Therefore, generous sample sizes should be employed whenever low cost per unit permits it.

Much more problematic than the risk caused by small sample sizes is the strong (4th to 7th power) dependence of wear-out life, hence reliability, on the severity of environmental conditions. Unqualified life-test data must therefore be viewed with skepticism, and generous safety margins must be applied to compensate for the risk caused by the uncertainty of conditions.

This will be discussed further in the next section. But it may be stated right here that this risk may be greatly reduced by conducting life tests under conditions which are *undoubtedly* more severe than those expected in service.

6. How Many Standard Deviations?

The question arises: How many standard deviations shall be specified? Actually, there is no fixed number to be specified for all types of components, relative to all environmental conditions and design criteria for the following reason: To assure that a component type will never cause the loss of complex military equipment, every conceivable risk factor, such as uncertainties of measurements, skills, and of war conditions, must be covered by a safety margin of its own. Figure 12 contains a tentative list of factors which must be considered in specifying safety margins that are really adequate.

The *total* contingency margin, K_c, may now be computed by simply adding up the various contingency margins. However, since not all of the contingencies will occur at the same time, or during the same firing, it suffices to take the square root of the sum of the squares, for example:

FACTORS INFLUENCING CHOICE OF SAFETY MARGINS	Specified Contingency Margin (Standard Deviations)
1. Uncertainty in Determining Service Conditions	1
2. Uncertainty in Predicting Design Parameters	2
3. Uncertainty of Test Methods	1
4. Uncertainty of Statistical Evaluations	1
5. Uncertainty in Judging Reliability Skills of Subcontractors and Vendors	2
6. Uncertainty in Judging Reliability Skills of Maintenance People	2
7. Risk of Two-Front System (See Reference 1, Part III)	3
8. Employment in Low-risk Equipment	0
9. Employment in High-risk Equipment	3
10. Employment in Ultrahigh-risk Equipm.	10
11. Non-destructive Testing Impractical	2
12. Redundant Usage Impractical	1
13. Saving of Weight *Not* an Iss.	2

Fig. 12. Suggested List of Contingencies and Contingency Margins

$$K_c = \sqrt{1^2 + 2^2 + 1^2 + 1^2 + 2^2 + 2^2 + 3^2}$$
$$\sqrt{5^2 + 2^2 + 1^2 + 2^2}$$
$$= \sqrt{58} = 7.6 \approx 8 \text{ standard deviations}$$

The basic principle of the total *contingency margin*, K_c, is that it be kept strictly in reserve just in case that any of the contingencies, or any combination of them, might occur in service. Therefore, to allow for the inherent, or "legitimate," variation of strength, an additional *scattermargin*, K_s, of say three standard deviations must be specified, as illustrated in Figure 13. (See Reference 1, Part I.)

Specifying and attaining the minimum contingency margin is the responsibility of the reliability engineer. He will have to keep all lists of contingencies and contingency margins on file so that he may check them in order to ascertain whether or not a failure was caused

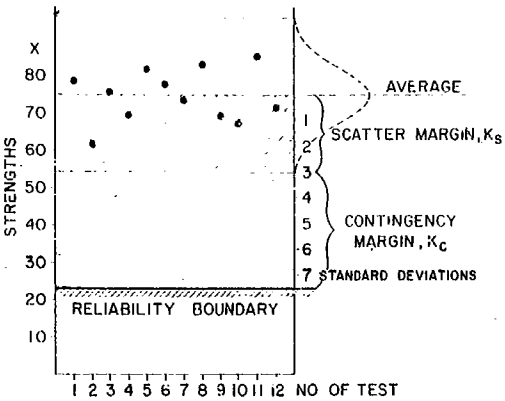


Fig. 13. Contingency Margin and Scatter Margin

by an inadequate specification. He may have to make an original specification more stringent if, for example, the reliability skill of a vendor, or of a maintenance crew is lower than he had anticipated. He may have to make a specification less stringent if, for example, a component turns out to be much heavier than expected, or if the cost of achieving and maintaining a specified safety margin turns out to be excessive.

Once a satisfactory degree of design reliability is established, and proved to exist by tests to failure, the quality control engineer will take over. He has the responsibility of assuring, by approved methods of statistical quality control, that during the manufacturing process neither the average strength decreases nor the standard deviation increases. He must prove this continuously by testing to failure small but adequate production samples with regard to those environmental conditions which, during the prototype tests, have shown the need of permanent control. In this manner, the quality control engineer may maintain, and even increase, the safety margins established in the prototype stage.

Compared to the old-fashioned method of specifying fixed safety *factors*, the procedure of safety margins described here might appear unnecessarily elaborate. It is not. When a component may cause the total loss of a million-dollar missile or aircraft, or the loss of lives, it is the first duty of the reliability engineer to carefully consider every conceivable contingency and to cover it by a generous safety margin of its own.

7. Overdesign and Reliability

It is often argued that generous safety margins unavoidably lead to *overdesign,* that is, to excessive weight, reduced performance, high cost, and delayed schedules. Is this true?

There is the performance fanatic who, by sacrificing reliability, economy and schedules, tries to squeeze out of his design the last mile per second, and the last foot of ceiling. There is the unresourceful, apprehensive designer who clings to his design, unable to finish and release it for production. In either case, warnings against overdesign are well justified.

But there is also the hasty, superficial designer who, *pretending to fight against overdesign,* tries to push a new design into production, be it mature or immature, light or heavy, inexpensive or expensive, reliable or unreliable.

Significantly, advocates of haste and superficiality are the ones who assert that reliability may be improved later, during production and service use, by quality control and failure reporting. Since this is impossible, they just bring about the very consequences of overdesign they pretend to battle, namely excessive weight, reduced performance, high cost and—as a result of necessary design changes—badly delayed schedules. Worst of all, they bring about poor reliability. This is why reliability engineers must take issue.

While warnings against overdesign are oftentimes justified, they must never be misconstrued as an invitation to neglect the principl of safety margins. Whenever this is the case, the Reliability Coordinator must take immediate action, educational or otherwise, before a low reliability barrier becomes chronic and incurable.

8. Statistical Accuracy and Reliability

Since component reliability is primarily a function of the design safety margin, and since we must strive for *absolute* component relia-

bility, the emphasis must be on *generous*. In specifying safety margins it would be unwise to be niggardly, particularly in the innumerable cases where large safety margins may be attained easily without adding weight, cost, and time. As stated before, 10 standard deviations are better for reliability than five, and 20 are better than 10. *Generosity in specifying safety margins is therefore the hallmark of the experienced reliability-conscious engineer (compare List of Safety Factors, Figure 2).*

Statisticians may argue that generous safety margins and statistical accuracy are not compatible. This is true. The purely statistical approach, whereby the "area under the tail" of a failure frequency distribution is accurately translated into probabilities of failure, or indices of reliability, will result in an overly optimistic judgment of reliability, hence in disaster. Looking at the list of risk factors, Figure 12, the reader will note that uncertainty of statistical evaluation is one of many contingencies, *but by no means the most hazardous one.* This proves that in matters of reliability, striving for statistical accuracy is futile. It is even dangerous because it may divert attention from the many other risk factors which, if not taken care of by generous contingency margins, may kill many more missiles than the hazard generated by the uncertainty of statistical evaluation.

9. Who Shall Write Reliability Specifications?

Which agency shall conceive and specify the size of the safety margins? Is it the prime contractor, or the contracting agency, or who?

As just discussed, the proper designation of safety margins must be based on a wide variety of engineering considerations. These, however, are known only to those who are thoroughly familiar with the details of the design of a component type, or an equipment, that is the designers, test engineers, and production engineers.

Unfortunately, we cannot expect that thousands of design specialists are equally and sufficiently conscious of the serious reliability problem of guided missiles and their components, arising as a result of the long chain of automatic devices. True, many might be genuinely reliability-minded, yet experience shows that the majority are not eager to fight for the cause of reliability. (In justice to them it should be said that oftentimes funds are not available to pursue the cause of reliability.) However, since any single designer, as a link in the reliability chain, may ruin a whole missile type, it should not be his prerogative to choose the minimum safety margins according to personal taste. Designating, specifying, and controlling safety margins should be the task of the assigned reliability organization of the prime R&D contractor. Such an organization should consist of highly skilled, highly reliability-minded design specialists in the various fields of technology, such as electronics, aerodynamics, hydraulics, servo-mechanisms, guidance systems, stress analysis, propulsion, warheads, inspection and quality control, logistics, and operational analysis.*

It thus becomes clear that the responsibility for writing of, and complying with, reliability specifications must be placed squarely on the shoulders of the R&D *prime contractor.*

10. The Role of Contracting Agencies

But this does not imply that contracting agencies shall have no responsibility in writing reliability specifications. True, such an agency must place a great deal of reliance on the integrity and reliability-mindedness of a prime contractor. However, since contracting agencies are immediately responsible to the Armed Forces and the taxpayer, they must not exempt themselves from establishing and controlling reliability policies. Rather, they must write a *Reliability Code,* specifying at least *minimum*

*In order to obtain competent reliability engineers it will be necessary to pay them salaries commensurate with the enormous difficulty and responsibility of their task, and to place them high in the organization. (For further discussion of the organization and tasks of a reliability coordination group see Reference 5, pages 39-44 and Reference 6, Section K.)

safety margins which the contractor must prove to exist.

This is nothing new. Wherever large material values and human lives are at stake, as in the design of buildings, elevators, and piloted aircraft, contracting agencies are, as a matter of course, forceful in conceiving, specifying and controlling generous safety factors. No contractor would dare ignore them and no contracting agency would accept a product which does not comply.

In Part IV an attempt is made to write a Reliability Code for guided missiles.

PART IV
RELIABILITY CODE FOR GUIDED MISSILES

1.1 *General*

Since guided missiles are fully automatic, and non-recoverable, the failure of any one component will result in the failure of the entire missile. In order to achieve an acceptable overall reliability, missile components must be made much more reliable than usual. Two or three times better than the commercial product is not nearly enough; they must be made perhaps a thousand times more reliable, or better, "absolutely" reliable.

To approach this goal, the following paragraphs are specified:

1.1.1 *Determining Overall Reliability*

The overall reliability of the missile system shall be ... per cent. To prove this, not less than ... missiles shall be fired at range of ... miles, under proving ground conditions, within the Ordnance Engineering-User Test Program. (Numerical values shall be specified depending upon the military characteristics of a missile; upon the cost per test firing, including all operational expenses; and upon the total number of missiles produced.)

1.1.2 *Homogeneity of Test Samples*

In determining the overall reliability of missiles, the contractor shall *not* be required to keep the sample homogeneous, just for the sake of statistical accuracy. Rather, he shall try to increase the reliability of the remaining missiles as much as possible by promptly redesigning or remanufacturing all types of components which, during the preceding test firings, have proved inadequate. Increasing reliability shall have priority over measuring reliability.

1.1.3 *Surveillance of Reliability*

The growth of reliability of the missile and its components shall be accelerated and controlled thoroughly and systematically by an organization of highly qualified reliability engineers.

1.1.4 *Missile Breakdown*

The missile system shall be broken down into its packaged units, subassemblies, components, and parts. The original breakdown lists, and subsequent revisions, shall be presented to the contracting agency for approval.

1.1.5 *Definitions*

a. *System:* A group of equipments integrated to perform a function. (Example: A weapon consisting of a missile, and all ground or aircraft equipment necessary to operate it.)

b. *Equipment:* A combination of assemblies which is capable of operation by itself. (Example: A guided missile, including all packaged units within the missile.)

c. *Assembly:* A group of subassemblies, combined and packaged in one housing. (Examples: An antenna tuner, radio transmitter, the nose cone of a missile.)

d. *Subassembly:* A commonly mounted group of components which may be subject to disassembly, but which is not capable of operation by itself. (Examples: An i. f. strip, a terminal board with components attached.)

e. *Component:* An item not normally subject to further disassembly. (Examples: Resistors, capacitors, tubes, potted or molded items.)

f. *Element:* A part of a component that cannot be removed without destroying the component. (Examples: A filament of an electron tube, a contact of a relay.)

Electronic components contribute most to the unreliability of guided missiles because they are complex in themselves; because they are rarely developed for the exceedingly severe conditions and requirements in guided missiles; and because they usually occur in missiles in very large numbers. Electronic equipment shall therefore be broken down and controlled with particular care.

1.1.6 ***Environmental Stresses***

Existing general specifications of environmental conditions shall be applied only if their validity for the specific missile has been proven by testing a sufficient number of units. (See also 1.1.13, 1.1.16, and 1.1.17.)

1.1.7 ***Fixed Environmental Conditions*** shall be determined and specified by military requirements such as climatic conditions, or required storage age. These are, therefore, identical with the Reliability Boundary. (For discussion of Reliability Boundary, see 1.1.8, and Ref. 1, pages 38-43.)

1.1.8 ***Self-Induced Environmental Conditions*** shall be determined by the prime contractor, through calculations, laboratory tests, and flight tests. To this group belong all self-generated stresses, such as shocks, vibrations, accelerations, and temperatures. The average value of these stresses, as well as their characteristic variation, shall be determined by testing sufficient numbers of units. The variation shall be expressed by the sample standard deviation. (About standard deviation, see Fig. 14.)

1.1.9 ***Determination of the Reliability Boundary***

A numerical stress level shall be established for all environmental conditions, such as shock, vibration, temperature, corrosive conditions; for all other critical design requirements such as frequencies, voltages, pressures, sensitivities, selectivities, elasticities, alignments, adjustments, mechanical and electrical tolerances; and for all maximum supply requirements, such as electronic, hydraulic, or pneumatic power supplies. This stress level shall be used as the basis for the selection or development of components that must be capable of operating under these conditions with absolute reliability. This stress level is called the "Reliability Boundary." It shall be determined by adding a safety margin of six (6) standard deviations to the *average* value of the measured environmental stress condition, or design requirements, as shown in Figure 14.

TEST NO.	STRESS DATA	DEVIATION FROM AVERAGE	
	X	x	x^2
1	22	2	4
2	28	4	16
3	18	6	36
4	26	2	4
5	21	3	9
6	25	1	1
7	23	1	1
8	30	6	36
9	23	1	1
10	24	0	0
	$\Sigma X = 240$		$\Sigma x^2 = 108$

Stress Average $\bar{X} = \frac{\Sigma X}{N} = 24$

Stress Std. Dev. $s = \sqrt{\frac{\Sigma x^2}{N}} = 3.3$

Std. Dev., Enlarged $s_{enl} = 1.27s = 4.3$
(see 1.1.15)

Rel. Boundary $X + 6s_{enl} = 24 + 26.5 = 50.5$

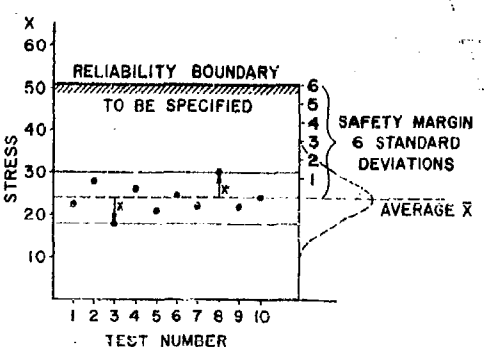


Fig. 14. Determining the Reliability Boundary

1.1.10 *Estimate of Environment*

Whenever a stress or design requirement has not yet been measured, a generously estimated value shall be established and used.

1.1.11 *Determination of the Strength of Components*

The strength of any type of component, relative to any environmental condition, or to any vital design requirement, shall be proved by testing to failure a sufficient number of units. (See also 1.1.14.)

TEST NO.	STRENGTH DATA	DEVIATION FROM AVERAGE	
	X	x	x^2
1	99	4	16
2	82	13	169
3	96	1	1
4	90	5	25
5	102	7	49
6	98	3	9
7	94	1	1
8	103	8	64
9	90	5	25
10	88	7	49
11	106	11	121
12	92	3	9
	$\Sigma X = 1140$		$\Sigma x^2 = 538$

Strength Average $\overline{X} = \frac{X}{N} = 95$

Strength Std. Dev. $s = \sqrt{\frac{\Sigma x^2}{N}} = 6.7$

Std. Dev. Enlarged (see 1.1.15) $s_{enl} = 1.24\,s = 8.4$

Strength Safety Margin $\frac{X - RB}{s_{enl}} = \frac{95 - 50.5}{8.4} = 5.2$ Std. Dev.

1.1.12 *Proof of Safety Margin*

The contractor shall prove that a safety margin of at least five (5) standard deviations is available between the average strength and the Reliability Boundary. (See Fig. 15.)

1.1.13 *Accelerating Test-to-Failure Programs*

Immediately after the preliminary design has been started, and the first component types

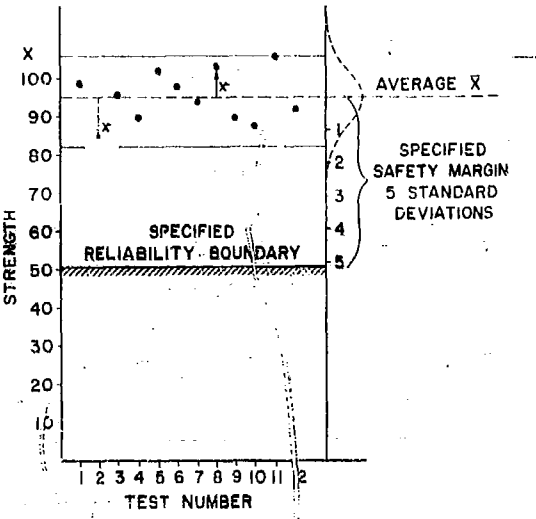


Fig. 15. Determining Component Safety Margin

tentatively selected, a vigorous test-to-failure program shall be started, and conducted with highest priority. Even where the severity of a condition or a design requirement is known only vaguely, or not at all, the contractor shall start failure testing of those types of components that may suffer from that condition. Once the condition and the Reliability Boundary are determined numerically, it can and shall be decided without delay whether or not the component type previously tested to failure is acceptable for use in the missile.

1.1.14 *Sampling for Failure Tests*

The number of units required for the individual test-to-failure programs may be small or large, as the case may be. The sample size shall be determined depending on these factors: the degree of maturity already achieved; the cost of the component; the cost and duration of one test; the number of units employed per missile; the complexity of the component; the complexity of the missile; and the importance of the missile to the national defense.

1.1.15 *Risk Factors for Small Sample Sizes*

The risk of accepting an unreliable component type increases as the sample size decreases.

To compensate for this risk, *and to stimulate the testing of generous sample sizes,* the sample standard deviation shall be enlarged by a risk factor obtained from Figure 16.

(For further discussion of sample risk factors, see Reference 1, pages 22-26.)

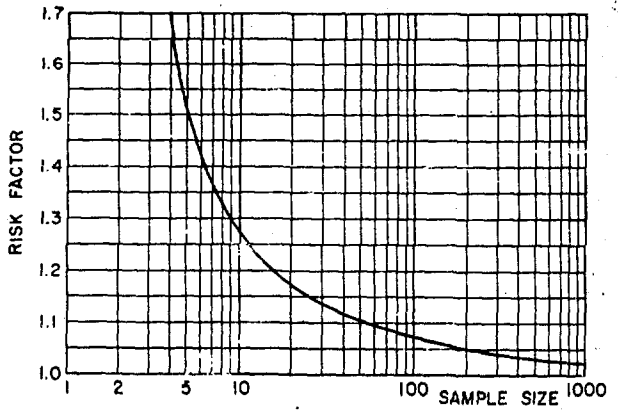


Fig. 16. Risk Factors Compensating for Small Sample Sizes

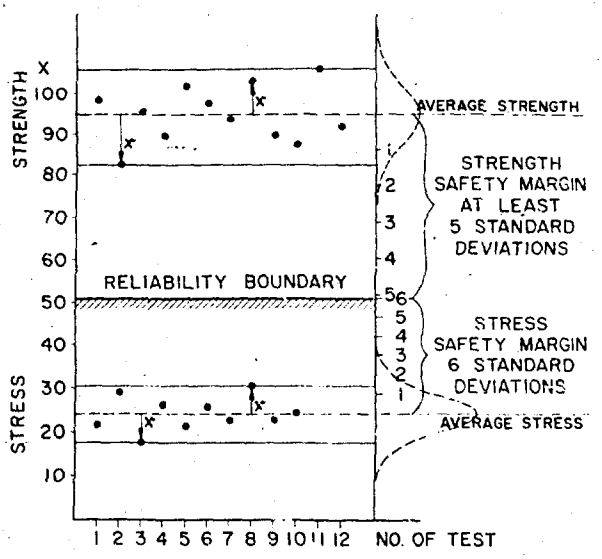


Fig. 17. Combination of Figs. 14 and 15 Illustrating How Scatterbands of Stresses and Strengths Shall be Separated by a Reliability Boundary

The enlarged standard deviation thus obtained shall be used to determine the safety margin, that is, the number of enlarged standard deviations available between the average strength and the Reliability Boundary. This is illustrated by the example in Figure 15.

1.1.16 ***The Relationship Between Scatterbands of Stresses and Strengths*** is illustrated in Figure 17. Because an error in determining a stress scatterband may ruin *many* component types, whereas an error in determining the strength endangers only *one* component type, the minimum *stress* safety margin shall be specified more generously (6s, for example) than the *strength* safety margin (5s, for example).

1.1.17 ***Safety Factors***

Whenever the first test-to-failure of a component type proves that it is at least four (4) times stronger than the Reliability Boundary, no further units need to be tested. A safety factor of four (4) may, in most instances, be considered as proof that, with regard to that particular condition, a high degree of reliability is already attained. If the contractor feels, however, that more units should be tested to failure to clarify the mechanics of failure, he may do so.

1.1.18 ***Relationship Between Safety Margins and Safety Factors***

A safety *factor* of four (4) is not a minimum requirement. It is intended to relieve the workload, cost, and schedule of a test-to-failure program whenever the first unit tested turns out to be at least four times stronger than the Reliability Boundary. In cases of simple, easily controllable components, showing safety factors of four and more, the reliability engineer may consider the component highly reliable in that particular respect, and discontinue the tests, at least for the time being. If, however, the strength of the first unit turns out to be *less* than four times the Reliability Boundary, particularly if the component is complicated and difficult to control, the contractor shall test more units and prove that a safety *margin* of at least five (5) standard deviations is available.

This relationship between the concept of safety factors and that of safety margins is

illustrated by the two examples of component types in Figure 18.

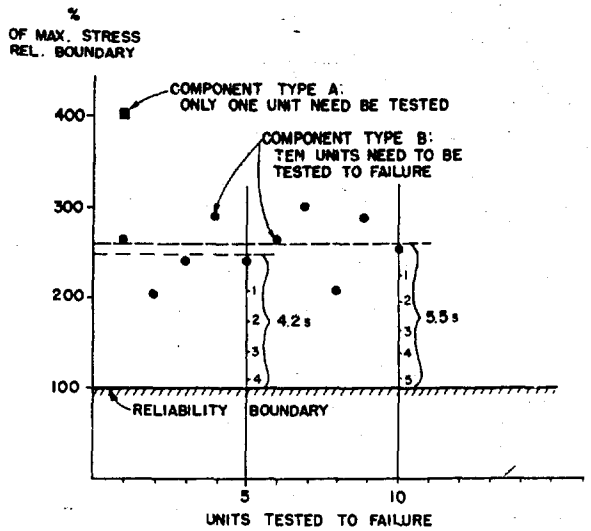


Fig. 18. Safety Factor Versus Safety Margin

In the case of component type A, where the first and only test proved a safety factor of four, no further units need be tested. In the case of component type B, where the first unit tested indicates a safety factor of only 2.7, the concept of safety *margins* must be employed. After having tested a total of five units, and having enlarged the sample standard deviation by the risk factor of 1.5 obtained from Figure 15, we may prove a safety margin of 4.2 standard deviations, which is not enough. We must test a few additional units, say five. This time, for a total of 10 test data, the sample standard deviation must be multiplied by a risk factor of only 1.27. Now the safety margin is 5.5 standard deviations and the component type may be accepted, as far as this particular condition or design criterium is concerned.

1.1.19 *Frequently Occurring Parts*

The safety margins and safety factors specified in the preceding paragraphs shall be applied and proved for component types that occur only once per missile. Since component types that occur more frequently constitute a proportionately greater hazard to the missile, the safety margins and factors shall be increased according to Figure 19.

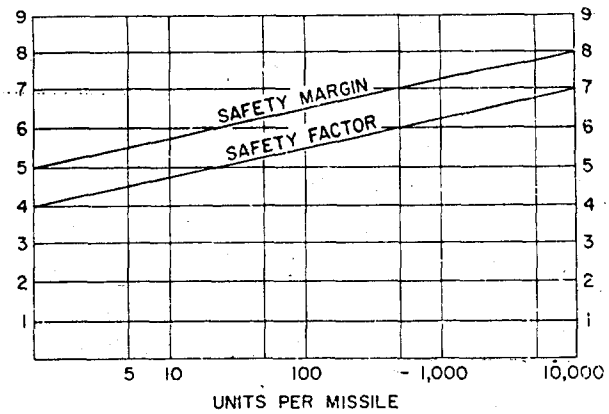


Fig. 19. Minimum Safety Factors and Safety Margins for Various Numbers of Units Employed per Missile

1.1.20 *Maintaining Reliability in Manufacture*

After the required "absolute" level of design reliability has been achieved for a type of component, it shall be maintained in manufacture by statistical quality control, and proved by repeating, as often as necessary, the essential failure tests on a sampling basis. However, the compromise between reliability and cost of reliability shall not be based on economic interests of the *contractor or vendor,* as in the commercial field, but rather on the military and economic needs of the *Armed Forces.* These needs are indicated by the fact that the failure of a 10-cent component may cause the total loss of a million-dollar missile.

1.1.21 *Waivers*

The safety margins specified in this code are minimum requirements. They must be attained and proved to exist before a missile type can be accepted for production. In the case of prototype missiles, fired for test purposes only, the contracting agency may permit employment of nonconforming components, provided that the contractor can prove that they will not contribute any risk to the test missile involved. For very complex and expensive missiles, this proof is absolutely required.

CONCLUSIONS

1. Since ordinary specif
inadequate to achieve the
component reliability requ
nents of guided missiles, th
mented by a special Reliabi
generous safety margins be
strengths.

2. Numerically defined
margins will be a strong inc
ing comprehensive reliabilit

3. Top management, de
neers, and manufacturers, k
is a hurdle to overcome, may
reliability-minded and may
implementation of a compre
program of guided missile
ponents.

4. Designers and test engi
pelled to determine the actu
conditions, rather than to
specifications which may be e

5. Designers and test engi
pelled to test their compo
failure, in sufficient number
termine the characteristic va
values, the modes of failure
margins attained.